

**REMARKS**

Claims 1, 3-7 are pending. Claim 2 has been cancelled. Claims 1, 3 and 5-7 have been amended to more clearly define the claimed invention.

Claims 1-7 have been rejected under 35 U.S.C. 103 as being unpatentable over Monier in view of Shimbo and further in view of Miura.

Claim 1 has been amended to further define the claimed invention. In particular, claim 1, as amended, recites, An encryption circuit, comprising:

- a plurality of operation circuits which are connected; and

- a control circuit dividing data to plural parts for providing to each of said plurality of operation circuits and controlling said plurality of operation circuits to provide encryption or decryption control.

Each of said plurality of operation circuits includes

- a first register holding corresponding part of data as operation data,

- an addition and subtraction circuit performing addition and subtraction with respect to the operation data held in said first register,

- a right-shift circuit performing right-shift with respect to an operation result by said addition and subtraction circuit, and

- a second register holding an operation result by said right-shift circuit.

The claim specifies that the addition and subtraction circuit in a first operation circuit performs addition and subtraction using a carry-in signal supplied from a second operation circuit, and outputs a carry-out signal as said carry-in signal of a third operation circuit.

Further, a right-shift circuit in said first operation circuit performs right-shift using a right shift-in signal supplied from said third operation circuit, and outputs a right shift-out signal as said right shift-in signal of said second operation circuit.

Also, the first operation circuit receives said carry-out signal from said second operation circuit before starting a calculation thereof, receives said shift-in signal from said third operation circuit during performing the calculation thereof, supplies said carry-out signal to said third operation circuit before starting the calculation of the third operation circuit, and supplies said shift-out signal to said second operation circuit during performing the calculation of the second operation circuit.

Hence, the claimed encryption circuit has a control circuit has a control circuit and a plurality of operation circuits. Each of the operation circuits includes the addition and subtraction circuit, right-shift circuit, and the first and second registers. The addition and subtraction circuit in one operation circuit (the first operation circuit) outputs the carry-out signal to the addition and subtraction circuit in another operation circuit (the second operation circuit), and the right-shift circuit in the one operation circuit outputs the shift-out signal to the right-shift circuit in the other operation circuit (the third operation circuit). The plurality of operation circuits cooperates using the carry-out signal and the shift-out signal.

Further, the first operation circuit receives the carry-out signal from the second operation circuit before starting a calculation thereof, receives the shift-in signal from the third operation circuit during performing the calculation thereof, supplies the carry-out signal to the third operation circuit before starting the calculation of the third operation circuit, and supplies the shift-out signal to the second operation circuit during performing the calculation of the second operation circuit.

The Monier, Shimbo and Miura references disclose the encryption/decryption circuit for calculating the RSA operation. These references disclose only a single operation circuit, not a plurality of operation circuits, as claim 1 requires.

The operation circuit disclosed in the references performs the loop operation for encrypting the initial data, and the carry-out signal and/or shift-out signal is transferred to the proceeding operation.

The references do not suggest using a plurality of operation circuits for encrypting the corresponding part of data, and the carry-out signal and/or the shift-out signal of one operation circuit is transferred to another operation circuit.

Further, the references do not disclose the timing of transferring the carry and shift signals between the operation unit. The Monier reference discloses the feedback loop from the addition circuit 31 to the subtract circuit 28 via the comparator 35 and the selector 37. But it does not disclose that the feedback signal via the selector 37 is received during the calculation of the subtract circuit 28 or the next calculation.

As stated in *Graham v. John Deere Co.* 383 U.S. 1, 13, 148 U.S.P.Q. 459, 465 (1966), obviousness under 35 U.S.C. §103 must be determined by (1) analyzing the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims in issue; (3) resolving the level of ordinary skill in the pertinent art, and (4) analyzing secondary considerations.

As demonstrated above, the combined teachings of the applied references do not disclose the features recited in claim 1. For example, the prior art do not disclose that the first operation circuit receives the carry-out signal from the second operation circuit before starting a calculation thereof, receives the shift-in signal from the third operation circuit during performing

the calculation thereof, supplies the carry-out signal to the third operation circuit before starting the calculation of the third operation circuit, and supplies the shift-out signal to the second operation circuit during performing the calculation of the second operation circuit, as claim 1 recites.

Hence, the invention of claim 1 is not obvious over the prior art teachings.

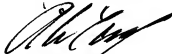
Claims 3-7 are defined over the prior art at least for the reasons presented above in connection with claim 1.

In view of the foregoing, and in summary, claims 1 and 3-7 are considered to be in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Alexander Y. Yampolsky  
Registration No. 36,324

600 13<sup>th</sup> Street, N.W.  
Washington, DC 20005-3096  
Phone: 202.756.8000 AVY:apr  
Facsimile: 202.756.8087  
**Date: May 12, 2008**

**Please recognize our Customer No. 20277  
as our correspondence address.**